

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 1 月 2 1 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 0 1 2 5 9 4

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

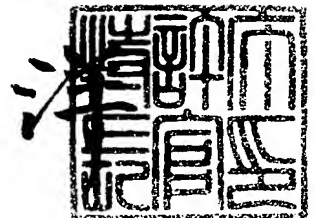
J P 2 0 0 4 - 0 1 2 5 9 4

出 願 人
Applicant(s): 株式会社日立製作所

2 0 0 5 年 5 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



・【官 規 則】	付 訂 願
【整理番号】	K03018151A
【特記事項】	特許法第30条第1項の規定の適用を受けようとする特許出願
【あて先】	特許庁長官殿
【国際特許分類】	G06K 19/077
【発明者】	
【住所又は居所】	神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内
【氏名】	加藤 崇利
【発明者】	
【住所又は居所】	神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内
【氏名】	常広 隆司
【発明者】	
【住所又は居所】	神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内
【氏名】	萱島 信
【発明者】	
【住所又は居所】	神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内
【氏名】	仲川 和志
【特許出願人】	
【識別番号】	000005108
【氏名又は名称】	株式会社 日立製作所
【代理人】	
【識別番号】	100075096
【弁理士】	
【氏名又は名称】	作田 康夫
【選任した代理人】	
【識別番号】	100100310
【弁理士】	
【氏名又は名称】	井上 学
【手数料の表示】	
【予納台帳番号】	013088
【納付金額】	21,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1

【請求項 1】

リモートアクセスシステムであって、
サーバと、
前記サーバにアクセスするクライアント機器と、
前記サーバと前記クライアント機器とを接続するネットワークと、
前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンバ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、
前記記憶媒体には、前記クライアント機器で、前記遠隔操作アプリケーション、前記暗号化アプリケーション、前記業務アプリケーションを動作させるミドルウェアが格納され、

前記クライアント機器のCPUは、前記ミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間で通信を行うことを特徴とするリモートアクセスシステム。

【請求項 2】

請求項 1 記載のリモートアクセスシステムであって、
前記ファイルアクセス用ドライバ、あるいは前記デバイスドライバからの命令が発生した場合、予め定めた順序で、前記命令を制御することを特徴とするリモートアクセスシステム。

【請求項 3】

請求項 2 記載のリモートアクセスシステムであって、
前記ファイルアクセス用ドライバ、あるいは前記デバイスドライバからの命令が発生した場合、前記デバイスドライバからの命令を優先して実行することを特徴とするリモートアクセスシステム。

【請求項 4】

請求項 1 記載のリモートアクセスシステムであって、
前記記憶媒体は、更に、一時記憶領域を有し、
前記クライアント機器で実行された処理により生じたデータを、当該一時記憶領域に格納することを特徴とするリモートアクセスシステム。

【請求項 5】

リモートアクセスシステムであって、
サーバと、
前記サーバに接続されたゲートウェイと、
前記サーバにアクセスし、前記ゲートウェイとの間で認証処理を行うクライアント機器と、

前記サーバと前記クライアント機器とを接続するネットワークと、
前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、業務アプリケーションと、耐タンバ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、

前記記憶媒体には、前記クライアント機器で前記遠隔操作アプリケーション、前記暗号化アプリケーション、前記業務アプリケーションを動作させるミドルウェアが格納され、
前記クライアント機器のCPUは、前記ミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間で通信を行うことを特徴とするリモートアクセスシステム。

、セヘシヘノム。

【請求項 6】

請求項 1 または 2 のいずれか記載のリモートアクセスシステムであって、 前記サーバは、複数のサーバと、当該複数のサーバに接続された制御装置を有し、

前記クライアント機器は、前記制御装置にアクセスし、前記複数のサーバの電源管理を行うことを特徴とするリモートアクセスシステム。

【請求項 7】

請求項 1 または 2 のいずれか記載のリモートアクセスシステムであって、
前記記憶媒体は、前記耐タンバ領域内に格納された認証情報のコピーを保持することを特徴とするリモートアクセスシステム。

【請求項 8】

サーバと、ネットワークを介し前記サーバにアクセスするクライアント機器と、前記クライアント機器に接続され、前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、耐タンバ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体とを有し、前記クライアント機器から前記サーバにアクセスするリモートアクセスシステムにおけるゲートウェイであって、

前記記憶媒体から前記クライアント機器にロードされるミドルウェアにより動作される、インターフェースハンドラ、デバイスドライバを介して送信される前記認証情報に基づき、前記クライアント機器を操作するユーザの認証処理を行うことを特徴とするゲートウェイ。

【請求項 9】

サーバにネットワークを介し接続されるクライアント機器であって、

前記サーバを遠隔操作する遠隔操作アプリケーションプログラムと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションプログラムと、耐タンバ格納領域に格納された前記サーバに対する遠隔操作のための認証情報とを有する記憶媒体が接続されるリーダライタを有し、

前記リーダライタを介し、前記記憶媒体からロードされるミドルウェアを実行し、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとの通信を行うことを特徴とするクライアント機器。

【請求項 10】

サーバと、ネットワークを介し前記サーバにアクセスするクライアント機器との間でリモートアクセスを行うためのプログラムであって、

前記クライアント機器にインストールされ、ファイルアクセスを行う場合、ファイルアクセス用アプリケーションインタフェース、ファイルアクセス用ドライバを動作させ、認証処理を行う場合、インターフェースハンドラ、デバイスドライバを動作させ、前記サーバとクライアント機器間の通信を実現させるためのプログラム。

【発明の名称】 セキュアリモートアクセスシステム

【技術分野】

【0001】

本発明は、サーバをネットワークを介して安全に遠隔操作することを可能にするセキュアリモートアクセスシステムに関する。特にクライアントを適切にサーバに接続する為の耐タンパデバイスとクライアントもしくは耐タンパデバイス上に記録するプログラム、及びリモートアクセスシステムを動作させるためのネットワーク接続技術に関する。

【背景技術】

【0002】

近年パーソナルコンピュータ（PC）やネットワーク機器の低価格化が進み、従業員の大半にPCのような業務利用する端末を配布し、業務を行わせるようにしている企業が多数を占めるようになってきている。PCが低価格化し、利用が増えると、企業内の機器管理者のメンテナンス作業を行う必要のあるPCの数も比例して増える。このメンテナンス作業とは、例えばオペレーションシステム（OS）や業務アプリケーションのバージョンアップやバグフィックス、ハードウェア的な障害への対応、ウィルス対策やウィルス駆除などが挙げられる。このようなメンテナンス作業を行う管理コストは非常に大きく、従業員数が増加すると、比例して莫大なものになる。

【0003】

この管理コストを低減するための一手法として、サーバクライアント方式と呼ばれるシステム運用の方式が取られている。これは、主なプログラムやデータをサーバ側に蓄積し、例えばThin Client（シンクライアント）のようなクライアント側に蓄積するデータを低減させたものである。

【0004】

サーバクライアント方式では、演算処理やデータの蓄積は主にサーバ側で行われるため、シンクライアントのようなクライアント側にて個々にOSや業務に利用するアプリケーションのバージョンアップやバグフィックス、ウィルス対策やウィルス駆除などを行う必要性や頻度が減少するため、全体の管理コストを低減できる。

【0005】

また、近年、ICチップと呼ばれるプロセッサをカード内に内蔵したICカード（別名スマートカード）が、電子認証機能をもつキーデバイスとして注目されている。ICカードとは、主に内部のICカードモジュールに中央演算処理装置（CPU）を内蔵しているカードのことを指す。ICカードのメモリにはROM、EEPROMなどが使用される。ICカードは、カード自身に演算機能を持つため、ホストからの読み書き指示の際、正しいユーザからアクセスが行われたものかどうか自身で判断する機能を持つ。また、CPU自体の偽造が困難であるため、耐タンパデバイスであるICカードモジュール（ICカードチップ）の発する情報の改ざんや、不正にICカードモジュール内部にアクセスすることが難しい。このため、高いセキュリティレベルを持つシステムを構築可能である。多くのICカードは、ユーザの登録した個人認証番号（PINコード）とカード内部に保持されたPINコードを照合するなどして、ICカード内の情報を適切にリーダライタ、もしくはホスト出力するか、もしくはしないか等の制御を行うことが可能である。ICカードは内部にEEPROMやRAMなどの書き換え可能なメモリを持ち、ユーザやカード発行者のアプリケーションや情報を格納することができる。ICカードは、外部から入力される情報に対し、その該当するカード内にしか存在し得ない情報（秘密鍵等）を用いた演算をするなどして、カード外部にカード所有者のみしか知りえない情報もしくは作りえない情報などを出力することでカード所有者を認証させたり、否認防止のための情報を出力したりすることが可能である。

【0006】

また、フラッシュメモリカードは、不揮発性のメモリモジュールを内蔵したメモリカードでユーザの情報をメモリカード内に記憶することが可能である。フラッシュメモリカー

トの多くは、第3者が自かつの攻撃に対するハードウェア的な耐久性（耐ノック性）を持っていない。耐タンパ性を持たないフラッシュメモリカードは、盗難、紛失時にカードが分解され、カード内のメモリもしくはコントローラを解析されることにより保持している情報が第3者に漏洩する可能性が少なくない。

【0007】

また、特許文献1に記載されるようにフラッシュメモリインターフェースとICカード機能を持つフラッシュメモリカードが開示されている。このフラッシュメモリインターフェースとICカード機能を持つフラッシュメモリカードは、その記憶容量の大きさから、パソコンやワークステーションに構築されたユーザの保管文書や設定ファイル等をカード内に保存して持ち歩くために都合がよい。

【0008】

【特許文献1】特開2001-209773号公報

【発明の開示】

【発明が解決しようとする課題】

【0009】

前述したサーバクライアント方式では、サーバとクライアントの間の認証やデータのやり取りはネットワークを介して行われる。このため、ネットワーク上の一つのクライアントから、サーバへのアクセスを行う際に、サーバ側ではアクセスしてきたクライアントが正しいクライアントであるか否か、またクライアントを利用している利用者が正しい利用者であるか否か等の検証作業を行う必要がある。

また、クライアント側でも、アクセスしているサーバが正しいサーバであるか否かを検証せずには自分が欲する業務を行うことができない。もし上記のような検証を行わないとサーバ側に蓄積したデータや、利用者の持つ情報が第3者に漏洩する可能性がある。そこで、ネットワーク上での認証や、業務遂行中の送信情報などの暗号化などのセキュリティを十分に高める必要がある。

【0010】

本発明の目的は、ICカードに実装されるICチップのような認定された耐タンパデバイスの中に利用者の認証情報を格納し、かつ、大容量のファイルを安全に格納し、持ち歩くことのできるフラッシュメモリカードのようなストレージデバイスを認証デバイスとするサーバクライアントシステムによりユーザの利便性を向上させることにある。

【0011】

また、そのサーバクライアントシステムに使用可能な認証用ストレージデバイスを提供することも本発明の目的である。

【0012】

本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【課題を解決するための手段】

【0013】

本願において開示される発明のうち代表的なものの概要を説明すれば、下記の通りである。すなわち、上記の目的を達成するために本発明に係るリモートアクセスシステムは、耐タンパデバイスとストレージとコントローラの機能を実装したストレージデバイスと、前記ストレージデバイスを接続するためのリーダライタと、前記リーダライタと接続するクライアントと、ネットワークを介し前記クライアントから遠隔操作されるサーバとネットワーク上の暗号通信を行うためのゲートウェイを具備し、前記ストレージの中に、前記サーバを遠隔操作するアプリケーションと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションを記録しており、前記ゲートウェイと前記クライアントの暗号通信を行うための認証情報を前記耐タンパデバイス内に格納していることを特徴とする。

【発明の効果】

【0014】

本発明によれば、認定された耐タンパデバイス搭載したストレージデバイスを利用者に

配布し、利用者がヘッドレッシングノックへを不特定のソフトウェアに接続し、ヘッドレッシングノック内の認証情報とアプリケーションを用いてサーバを遠隔操作するサーバクライアントシステムを提供することにより、利用者の使い勝手を向上することが可能で、結果としてシームレスに職場内外での業務遂行機能を利用でき、かつ操作したクライアント内に残る機密情報を低減することにより、ユーザのクライアント利用時のセキュリティ及び利便性を向上させるリモートアクセスシステムを提供できる。

【発明を実施するための最良の形態】

【００１５】

本発明の実施の形態について、添付図面を参照しながら以下詳細に説明する。なお、図面中にて同一の参照番号を付したものは、同一の機能を有する構成要素を示し、説明の便宜上、その詳細な説明は省略する。

【実施例１】

【００１６】

図１から図７を用いて、本発明に係るセキュアリモートアクセスシステムの第１の実施形態を説明する。

【００１７】

図１は、本発明の第１の実施形態を示すリモートアクセスシステムを示す図である。

【００１８】

利用者の使用するサーバ１０００と複数のクライアント（クライアント１００１及びクライアント１００２）は、ネットワークケーブル１００３、１００４及び１００５を介し、ネットワーク１００６に接続されている。ネットワークケーブル１００３、１００４及び１００５とネットワーク１００６は、図示しないネットワークハブやスイッチにて適切に接続され、ネットワークケーブル１００３、１００４、１００５及びネットワーク１００６上の接続された機器へのパケットのルーティングが適切に行われ、正常に通信が可能な状態にある。サーバ１０００は、図示しないディスプレイインターフェースを通してディスプレイ１００７と接続されている。クライアント１００１及び１００２も同様に図示しないディスプレイインターフェースを介してそれぞれディスプレイ１００８及び１００９と接続されている。クライアント１００１及び１００２にはそれぞれユーザインターフェース１０１０及び１０１１が接続されている。ユーザインターフェース１０１０及び１０１１はキーボードやマウス、トラックボール、タッチパネル、タッチパッド、指紋リーダ、生体情報読取装置などにより構成される、クライアント１００１及び１００２の利用者の入力情報をそれぞれクライアント１００１及び１００２に送信する機能を持つ。

【００１９】

リーダライタ１０１２及び１０１３はそれぞれクライアント１００１及び１００２に接続されており、ストレージデバイス１０１４を挿入する機能を持つ。ストレージデバイス１０１４内の後述する端子２０００はリーダライタ１０１２の図示しない端子と接続され、クライアント１００１と通信を行うことができる。ストレージデバイス１０１４は利用者が携帯し持ち歩くことが可能で、クライアント１００１以外の例えばクライアント１００２のような機器においても利用が可能な設計となっている。

【００２０】

ストレージデバイス１０１４は、内部にコントローラ１０１５、耐タンパデバイス１０１６、ストレージ１０１７を実装している。コントローラ１０１５、耐タンパデバイス１０１６、ストレージ１０１７はそれぞれ別の集積回路として実装されているように記載されているが、機能をまとめた１つの集積回路として実装しても良い。耐タンパデバイス１０１６は例えばＩＣカードチップなどのセキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。

【００２１】

サーバ１０００内部には、ＣＰＵ１０３０、メモリ１０３１、ストレージ１０３２が実装されている。クライアント１００１には、ＣＰＵ３０００、メモリ３００１、ストレージ３００２、クライアント１００２には、ＣＰＵ１０５０、メモリ１０５１、ストレージ

１００２が示されている。

【００２２】

CPU1030上にて実行される情報は、通常ディスプレイ1007により表示されるが、サーバクライアント型の処理を要求する接続がクライアント1001よりサーバ1000に行われ、認証が確立し、サーバ1000とクライアント1001の遠隔操作の暗号通信が確立した場合、クライアント1001を介してサーバ1000上でプログラムを実行した処理結果はディスプレイ1008に表示される。この際、ディスプレイ1008上に表示される情報は、ディスプレイ1007に表示される情報と表示方法を同一にしてあり、ユーザは、クライアント1001とユーザインターフェース1010を利用しているのと、サーバ1000を直接操作しているのと同様に感じ取るため、利用者のユーザビリティを高めることができる。

【００２３】

図2にストレージデバイス1014の詳細を示したブロック構成図を示す。ストレージデバイス1014は、端子2000、コントローラ1015、耐タンパデバイス1016、ストレージ1017を実装しており、それぞれが図示するように接続されている。コントローラ1015は内部にCPU2001、メモリ2002、不揮発メモリ2003、インターフェース(I/F)2004、2005、2006を持つ。ストレージ1017は、フラッシュメモリ、ハードディスク、EEPROM、MRAM、MO、光ディスク等の不揮発性の記憶媒体である。本実施例においては、ストレージ1017がフラッシュメモリであるという前提において説明を行うが、他の種類の記憶媒体であっても良い。

【００２４】

コントローラ1015内のCPU2001は、不揮発メモリ2003からメモリ2002にロードされたアプリケーションを実行し、ストレージ1017のファイル管理や耐タンパデバイス1016のリセットや制御等の、耐タンパデバイス1016及び端子2000及びストレージ1017の間の通信の管理をI/F2004～2006を介して行う。

【００２５】

不揮発メモリ2003は、公開鍵演算プログラム2050、共通鍵演算プログラム2051及びストレージ1017内のファイル管理プログラム2052を含む。また、不揮発メモリ2003は、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持っていてもよい。

【００２６】

耐タンパデバイス1016は、内部にCPU2030、メモリ2031及びストレージ2032を含む。コプロセッサ2033はCPU2030の演算機能のうち暗号機能などの補完するコプロセッサであるが、CPU2030の計算速度が高速である場合、実装しなくてもよい。CPU2030は、ストレージ2032からメモリ2031にロードされたアプリケーションを実行し、後述する共通鍵による暗復号、非対称鍵による暗復号、ストレージ2032内のファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持つ。耐タンパデバイス1016は、電圧変動などの様々な攻撃に対して強い耐性のある、セキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。

【００２７】

ストレージ2032は、EEPROM、MRAM、フラッシュメモリなどの不揮発性ストレージである。ストレージ2032は、内部に秘密鍵2040、PIN情報2041、ログ情報2042、証明書2043、公開鍵2044、PIN検証プログラム2045、鍵証明書格納プログラム2046、公開鍵演算プログラム2047、共通鍵演算プログラム2048、鍵生成プログラム2049等を保存する。保存されたプログラムは、1つでも複数でも良い。ストレージ2032内のデータやプログラムは、メモリ2031にロードされ、CPU2030を動作させたり、コントローラ1015を経由して耐タンパデバイス1016外部に送信される。

【００２８】

秘密鍵２０４０は、利用者の認証や通信路を暗号化するための鍵であり、１つでも複数個でも良い。秘密鍵２０４０は、対応する鍵アルゴリズムの種類によって異なるフォーマットにて記述される。秘密鍵２０４０内の一つの秘密鍵に対応する公開鍵の集まりが公開鍵２０４４であり、対応する証明書の集まりが証明書２０４３である。証明書２０４３は、秘密鍵２０４０に対応する公開鍵２０４４の証明書であり、サーバ１０００や外部の認証局より発行されたものである。また、証明書２０４３は公開鍵２０４４の証明書とその他の証明書を発行した証明期間のルート認証局や中間認証局の証明書などその他の認証情報を含む。証明書２０４３のフォーマットは例えば国際電気通信連合（ITU）の定めるX.509の仕様を満たすものである。証明書２０４０内に格納される情報は、公開鍵と公開鍵に対する署名の他に、例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名や電子メールアドレスなどの利用者の情報及び拡張領域といった項目によって構成される。証明書２０１０はカード内からクライアント１００１及び１００２、サーバ１０００内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【００２９】

PIN情報２０４１は、耐タンパデバイス１０１６外部から耐タンパデバイス１０１６内部の情報を出力させたり、演算を行わせたりする利用者の権利を検証するための情報である。PIN情報２０４１は、暗証番号（PINコード）でも良いし、パスフレーズと呼ばれるような桁数の長い文字列でも良いし、指紋、虹彩、顔形、声紋、静脈などによる生体認証の根拠となる生体認証情報でも良い。

【００３０】

ログ情報２０４２は、耐タンパデバイス１０１６の利用履歴が記録されたもので、CPU3000もしくは２００１もしくは２０３０が動作するたびに追記されたり、耐タンパデバイス１０１６の外部から適切な権利を持つ利用者が追記したり、読み出したりする。ログ情報２０４２は、第三者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【００３１】

PIN検証プログラム２０４５は、PIN情報２０４１が耐タンパデバイス１０１６外部から検証用に入力されたPIN情報と合致するか検証するプログラムである。検証結果が正しければ、耐タンパデバイス１０１６は利用者が内部の情報や演算資源を利用可能な状態にする。PIN検証プログラム２０４５は、ストレージ２０３２内にあり、メモリ２０３１にロードされるプログラムやストレージ２０３２上に保存される情報ごとに利用権限を定め、個別に認証を行う。例えば、耐タンパデバイスが通電された後の利用時に一度PIN検証プログラムにて正しいと判断された利用者には以降のアクセスにてPIN検証を求めなかったり、利用のたびにPIN検証を行ったりできるよう設定することができる。

【００３２】

鍵証明書格納プログラム２０４６は、ストレージ２０３２内に保存されている秘密鍵２０４０や公開鍵２０４４や証明書２０４３を耐タンパストレージ１０１６外部へ出力したり、耐タンパストレージ１０１６外部から内部へ取り込んでストレージ２０３２内に格納したりする機能を持つ。鍵証明書格納プログラム２０４６を利用するためにはPIN検証プログラム２０４５による検証が終了する必要がある。ただし、証明書２０４３や公開鍵２０４４を出力するだけであるなら、PIN検証プログラム２０４５による検証が不要としても良い。鍵証明書格納プログラム２０４６は、外部へ鍵や証明書を入出力する際に外部のCPU3000もしくは２００１もしくは２０３０とセッション鍵を交換し安全な暗号化通信路を設けて鍵や証明書をやり取りする機能を持っている。

【００３３】

公開鍵演算プログラム２０４７及び共通鍵演算プログラム２０４８は、それぞれ前述の公開鍵演算プログラム２０５０及び共通鍵演算プログラム２０５１と同様の機能を持つ。鍵生成プログラム２０４９は、秘密鍵２０４０及び公開鍵２０４４のうちの１つの鍵のベ

、非対称鍵の秘密鍵（六通鍵）を生成する機能を持つ。生成された公開鍵や六通鍵はストレージ2032内に保存されたり、外部に出力される。非対称鍵の秘密鍵は、秘密鍵2040内に保存される。

【0034】

ストレージ1017は内部に利用者を識別するための証明書2010、利用者がストレージデバイス1014を利用して操作を行ったログ情報2011、デバイスアクセス用ライブラリ2012、デバイス管理用ツール2013、デバイスドライバ2014、インターフェースハンドラ2015、インストーラ2016、遠隔操作端末用アプリケーション2017、暗号化通信路構築用アプリケーション2018、業務アプリケーション2019、一時記憶領域2020、認証情報のコピー2021を記録している。

【0035】

証明書2010は、クライアント1001やサーバ1000が利用者やストレージデバイス1014を識別する演算を行うために利用する。証明書2010のフォーマットは例えばITUの定めるX.509の仕様を満たすものなどであればよい。証明書2010内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書2010はストレージデバイス1014内やクライアント1001、サーバ1000内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【0036】

ログ情報2011は、利用者がストレージデバイス1014を利用して操作を行った際に、CPU2001もしくはCPU2030もしくはクライアント1001もしくはサーバ1000の指示により更新される。ログ情報2011は、サーバ1000上のアプリケーションやクライアント1001上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報2011は、第三者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【0037】

デバイスアクセス用ライブラリ2012は、クライアント1001にて動作する複数のアプリケーションがストレージ1017にアクセスする際に利用する、ファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等の機能を利用するための関数群である。通常、後述するインストーラ2016によって、クライアント1001にインストールされて利用するが、直接、デバイスアクセス用ライブラリ2012がクライアント1001上のアプリケーションから利用されても良い。

【0038】

デバイス管理用ツール2013は、ストレージデバイス1014を管理するためのツールであり、例えば、利用者の認証番号を変更するツールや閉塞したストレージデバイスを初期化するツールやストレージデバイス上のプログラムやファームウェア、鍵情報、証明書の書き換えツールや、ストレージデバイス1014をデバッグする際に必要となるデバッグ用のモニタリングツールや、ストレージデバイスのマニュアルやヘルプファイルや、遠隔地からサーバの電源を投入するWake up on LANのような機能などを利用しクライアント1001やサーバ1000をリモートから電源投入や電源遮断をする電源管理するツールを含む。デバイス管理用ツール2013は、後述するインストーラ2015によりクライアント1001にインストールされても良いし、利用者がクライアント1001へ直接ロードして利用しても良い。

【0039】

デバイスドライバ2014は、ストレージデバイス1014の動作に必要な情報をOSに提供したり、動作を管理するプログラムであり、後述するインストーラ1015によりクライアント1001にインストールされる。

【0040】

インストーラ2014は、クライアント1001やサーバ1000上で動作するアプリケーションとデバイスドライバ2014を接続させる役割を果たす。

【0041】

インストーラ2016は、ストレージ1017上に存在するアプリケーションや情報、ドライバなどをクライアント1001やサーバ1000にインストールする際に利用者が利用する。インストーラ2016によってインストールされるアプリケーションや情報、ドライバ等は、インストール終了後に削除されても良いが、利用者が別の機器に接続してストレージデバイス1014を利用する際のためにストレージデバイス上に保存しておく。

【0042】

遠隔操作端末用アプリケーション2017は、クライアント1001からサーバ1000を遠隔操作するために利用する。遠隔操作端末用アプリケーション2017は、ターミナルサービスやリモートデスクトップ等といったクライアント1001やサーバ1000のOSの持つ標準のサービスやアプリケーションでもよい。遠隔操作端末用アプリケーション2017は、インストーラ2016によってクライアント1001にインストールされて利用されるか、もしくはストレージデバイス1014からクライアント1000に直接ロードされて利用される。

【0043】

暗号化通信路構築用アプリケーション2018は、クライアント1001とサーバ1000との間の通信を暗号化させるために利用される。暗号化通信路構築用アプリケーション2018は、サーバ1000とクライアント1001の間で秘密鍵を共有させ、その秘密鍵を用いることによりサーバ1000とクライアント1001の間に暗号化通信路を成立させる。この秘密鍵の共有に耐タンパデバイス1016内の秘密鍵等の秘密情報を用いてもよいし、秘密鍵を共有するプロセス内に耐タンパデバイス1016内の秘密情報を用いた認証を用いても良い。

【0044】

業務アプリケーション2019は、利用者がクライアント1001を利用する際に利用するアプリケーションである。業務アプリケーション2019は、例えばサーバ上のウェブベースのアプリケーションを利用するのであれば、ウェブブラウザであり、データベースを利用するのであれば、データベース操作用クライアントである。

ストレージ1017上の全ての情報が、耐タンパデバイス1016内にある秘密鍵2040のうちのいくつかの秘密鍵かサーバ1000もしくはクライアント1000上に保持する秘密鍵のうちのいくつかによって暗号化されていてもよいし、平文で記録されていてもよい。前者であれば、利用者に提供するセキュリティが向上する。また、コントローラ1015や耐タンパデバイス1016内において利用者認証が済んでいないとストレージ1017にアクセスできないようになっている場合、利用者に提供するセキュリティが向上する。

【0045】

一時記憶領域2020は、業務アプリケーション2019等のアプリケーションをクライアント1001上で実行するときに、アプリケーションの作成する一時ファイルを保存しておく領域である。業務アプリケーション2019やサーバ1000もしくはクライアント1001上の業務遂行用アプリケーションは、ビットマップのキャッシュなどの一時記憶ファイルを一時記憶領域2020内に作成する。一時記憶領域が暗号化されていない場合、利用者が利用を停止する際には、コントローラ1015もしくはクライアント1001上のOSもしくはアプリケーションの指示により一時記憶ファイルは消去される。このことにより、利用者の作成する一時ファイルはストレージデバイス上に記憶され、クライアント1001内の情報が第三者によって危険にさらされても利用者の利用した情報は安全に保護され、電源を切断したクライアント1001からの利用者の機密情報やプライバシーを含んだ情報はより漏洩しにくくなる。

図 1 2 にストレージ 1 0 1 7 上に記録された業務アプリケーション 2 0 1 9 やクライアント 1 0 0 1 などにインストールされたアプリケーションから一時記憶領域 2 0 2 0 を利用する際の処理方法をフローチャートにて示した図を示す。図 1 2 のフローチャートに示される処理は、アプリケーションの実行される CPU 1 0 3 0、もしくは 3 0 0 0 において行われる。例えば、遠隔操作端末用アプリケーション 2 0 1 7 や業務アプリケーション 2 0 1 9 は、CPU 3 0 0 0 上にて実行され、サーバ 1 0 0 0 上のアプリケーションは、CPU 1 0 3 0 上で実行されることになる。この際、利用者が利用するアプリケーションが起動される（1 2 0 0 0）と、一時記憶領域 2 0 2 0 がアプリケーションに定義されているかどうかと利用可能かどうか調べられる（1 2 0 0 1）。処理 1 2 0 0 1 において未定義もしくは利用不可能の場合一時記憶領域 2 0 2 0 の領域の定義と利用可能化（1 2 0 0 2）が行われる。次に、一時記憶領域の容量が十分かなど利用可能かどうかのチェックが行われる（1 2 0 0 4）。容量不足等の問題が検出された場合は容量不足など問題解決処理が行われ（1 2 0 0 5）異常状態から復帰できれば（1 2 0 0 6）処理が継続されるが、出来ない場合は、アプリケーションは異常終了する（1 2 0 0 7）。次にアプリケーションの処理が開始され（1 2 0 0 3）、一時記憶領域 2 0 2 0 への入出力が行われる（1 2 0 0 8）。アプリケーションの処理が継続されるようであれば、処理 1 2 0 0 4 へ戻る。アプリケーションが終了される場合、一時記憶領域 2 0 2 0 への入出力 1 2 0 1 0 が行われる。処理 1 2 0 1 0 はアプリケーションの利用した情報の消去とその確認作業である。処理 1 2 0 1 0 により利用者の利用した情報が適切に保全されたり、多くの場合は諸居されることにより、利用者の持つプライバシーを含む情報や秘匿情報が保護される。異常が無ければ、アプリケーションは終了する（1 2 0 1 1）。

【 0 0 4 7 】

アプリケーションによって、一時記憶領域 2 0 2 0 の定義方法がいくつか存在する。一つの方法は、アプリケーションが起動される際に、利用者ごとにクライアント 1 0 0 1 上に設けられた利用者のプロファイルに記載されてある一時記憶領域の設定をアプリケーションが読み込むことにより、一時記憶領域 2 0 2 0 の場所をアプリケーションが特定するやり方である。この際、利用者のプロファイルは、OS もしくはアプリケーションによって定義される利用者の設定情報で、ストレージ 3 0 0 2 もしくは、ストレージ 1 0 1 7 に記録されている。もう一つの方法は、アプリケーションが起動される際に、利用者に対し、OS もしくはアプリケーションがダイアログなどの確認手段をディスプレイ 1 0 0 8 上に表示するなどして、利用者に入力を促し、アプリケーションが一時記憶領域の設定を特定することである。この確認手段は多くはアプリケーションの最初の起動時に行われるが、毎起動時に行われても良い。以上のいずれかの方法によりアプリケーションは利用者の利用環境に対応した一時記憶領域の設定を行う。一度利用者が定義した情報は、クライアント上のストレージ 3 0 0 2 もしくはストレージ 1 0 1 7 上に情報を記録することにより、アプリケーション起動時にアプリケーションが再度利用すればよい。

【 0 0 4 8 】

認証情報のコピー 2 0 2 1 は、耐タンパデバイス 1 0 1 6 内にある例えば、証明書 2 0 4 3 や公開鍵 2 0 4 4 のような認証情報のコピーである。この認証情報のコピー 2 0 2 1 は、耐タンパデバイス 1 0 1 6 内にある公開鍵 2 0 4 4 や証明書 2 0 4 3 や PIN 情報 2 0 4 1 等のコピーである。

【 0 0 4 9 】

図 3 に認証情報のコピー 2 0 2 1 の例を示す。証明書 1（5 0 0 1）～証明書 N（5 0 0 3）は証明書 2 0 4 3 の一部である。ミドルウェアの認証情報 5 0 0 4 は、サーバ 1 0 0 0 もしくは、クライアント 1 0 0 1 のミドルウェアが認証情報のコピーが改ざんされていないかを検査するハッシュ値と署名やミドルウェアのバージョン情報、認証情報のコピーの作成された時刻情報などのミドルウェアの認証情報が含まれる。

【 0 0 5 0 】

一般的に耐タンパデバイス 1 0 1 6、コントローラ 1 0 1 5 間の通信速度はストレージ

クライアント1001、コントロール1001間の通信速度より遅いことが多い。このため、クライアント1001上のOSもしくはアプリケーションが耐タンパデバイス1016内の認証情報をストレージ1017にキャッシュもしくはコピーしておくことにより、利用者がストレージデバイスを利用する際に証明書2043の読み出しに要する時刻を短縮することができ、ユーザビリティを向上させることができる。認証情報のコピー2021は、ストレージデバイス1014が利用されるたびの検証されることが望ましく、その際に、認証情報のコピー2021の中の、ハッシュ値や耐タンパデバイス1016内の秘密鍵による署名や、クライアント1001上のOSもしくはアプリケーションによる署名が利用される。

【0051】

図4にクライアント1001の詳細を示したブロック構成図を示す。クライアント1001は、内部にCPU3000、メモリ3001、ストレージ3002、インターフェース(I/F)3020、3021、3022、3023を持つ。ストレージ3002は、フラッシュメモリ、ハードディスク、EEPROM、MRAM、MO、光ディスク等の不揮発性の記憶媒体である。

【0052】

CPU3000は、ストレージ3002からメモリ3001にロードされたアプリケーションを実行し、ディスプレイ1008、ネットワーク1006、ユーザインターフェース1010、リーダライタ1012との通信をそれぞれ、I/F3020、3021、3022、3023を介して行う。

【0053】

ストレージ3002は、証明書3010、ログ情報3011、デバイスアクセス用ライブラリ3012、デバイス管理用ツール3013、デバイスドライバ3014、インターフェースハンドラ3015、遠隔操作端末用アプリケーション3016、暗号化通信路構築用アプリケーション3017、業務アプリケーション3018が保存される。

【0054】

証明書3010は、クライアント1001やサーバ1000が利用者やストレージデバイス1014を識別する演算を行うために利用する。証明書3010のフォーマットは例えばITUの定めるX.509の仕様を満たすものなどであればよい。

【0055】

証明書3010内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書3010はストレージデバイス1014内の証明書2043やストレージ1017内の証明書2010のコピーや独自に利用者が登録した利用者や証明書を証明するルート認証局や中間認証局やストレージデバイス1014などの耐タンパデバイスの証明書であり、クライアント1001、サーバ1000内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【0056】

ログ情報3011は、利用者がクライアント1001の操作を行った場合に、CPU3000もしくはサーバ1000の指示により更新される。ログ情報3011は、サーバ1000上のアプリケーションやクライアント1001上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報3011は、第三者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【0057】

図5に利用者がクライアント1001にストレージデバイス1014を挿入し、サーバ1000を利用する際の利用者、ストレージデバイス1014、クライアント1001、サーバ1000間にて行われる通信の詳細を示した図を示す。利用者はクライアント1001の利用を開始するまでに利用者の認証情報やクライアント1001を動作させるためのアプリケーションが保存されたストレージデバイス1014をクライアント1001の

サーバーノードに接続する。利用者が、クライアント1001を利用したことがない場合は、利用者はストレージデバイス1014内のインストーラ2016を利用し、デバイスドライバ2014やデバイス管理ツール2013や遠隔端末用アプリケーション2017のようなサーバ1000を操作するために必要な情報もしくはアプリケーションをクライアント1001にインストールする。この際、クライアント1001によってストレージデバイス1014から直接実行できるアプリケーションのインストールを行う必要はない。

【0058】

利用者は、まずシーケンス4000に示すようにクライアント1001に動作確認要求を行う。クライアント1001はサーバ1000にサーバ動作確認を行う(4001)利用者はサーバ1000の動作を確認できなかった場合は、ストレージデバイス1014上のもしくはインストーラ2016にてクライアント1001上に用意された遠隔地からサーバの電源を投入するローカルエリアネットワーク(LAN)を利用して機器の電源投入を行うようなWake up on LANのような機能を利用してサーバ1000の電源投入を行う。この場合、サーバ1000の、ネットワークに対するI/Fのみは常時通電されており、IDとパスワードのセットやネットワークボードのMACアドレス等、何らかの認証情報を利用してサーバ1000の起動が行われる(4002、4003)。この操作によりサーバ1000は起動される(4004)。サーバの起動が完了した際、利用者はクライアント1000にログイン要求を入力する(4005)。クライアント1000内に遠隔操作アプリケーション2017及び暗号化通信路構築用アプリケーション2018がインストールされていない場合、この時点にてクライアント1001にロードされる(4006)。次にクライアント1001からサーバ1000にログイン要求が行われる(4007)。サーバ1000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証において公開鍵インフラストラクチャ(PKI)を用いた認証が必要もしくは可能である場合、サーバ1000からの認証情報の要求(4008)、クライアント1000からの証明書の要求(4009)、ストレージデバイス1014からの証明書の送信(4010)、クライアント1001からの署名の要求(4011)が行われる。ストレージデバイス1014において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。

【0059】

本実施例では、暗証番号を利用した例を示す。ストレージデバイス1014からの暗証番号要求(4012)が行われた後、クライアント1001から利用者へ暗証番号要求表示4013がディスプレイ1008などを利用して行われる。利用者が暗証番号をユーザーインターフェース1010とクライアント1001を介してストレージデバイス1014に送信すると(4014、4015)、ストレージデバイス1014内のCPU2001もしくはCPU2030においてサーバ1000、クライアント1001から送信された情報に対し、秘密鍵2040のうちの一つもしくはいくつかを用いた電子署名が作成される(4016)。作成された署名は、クライアントに送信される(4017)。クライアント1001は、証明書2010、2043などの認証情報と作成された署名の送信を行う(4018)。次に、サーバ1000及びクライアント1001は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う(4019)。この鍵交換4019は、遠隔操作端末用アプリケーション2017か暗号化通信路構築用アプリケーション2018により行われる。シーケンス4019において交換された秘密共有鍵を用いて、サーバ1000及びクライアント1001は暗号化通信路を構築し、2者の間で通信される情報は暗号化される。暗号化通信路が構築された段階で、ユーザは、サーバ1000または、クライアント1001、ストレージデバイス1014上に保存されているアプリケーションを起動し、業務遂行をする(4020)。

【0060】

業務遂行中は、CPU2001もしくはCPU2030もしくはサーバ1000もしくはクライアント1001は、ログ情報2011、2042、3011に情報を追記し、利

・利用者の乗初途11を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス1014やクライアント1001内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ1000に送信される。

【0061】

利用者の利用するサーバ1000の管理を行う管理者は、ログ情報2011、2042、3011の情報とサーバ1000に送信される情報を監査し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク1006を介した異常なアクセス、クライアント1001内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションとは、サーバ1000及びクライアント1001への利用者のログインの禁止や電源遮断、ストレージデバイス1014の閉塞などが該当する。ストレージデバイス1014の閉塞とは、PIN検証プログラム2045の利用する情報を変更し、利用者がストレージデバイス1014を利用できないようにすることである。

【0062】

利用者の業務など、サーバ1000の利用が終了した場合、利用者は、クライアント1001に対しサーバ遮断要求を行う(4021)。サーバ遮断要求はクライアント1001からサーバ1000に送信される(4022)。サーバ1000及びクライアント1001はセッションの遮断4023を行う。サーバ1000は、利用者の利用情報のログをサーバ1000上に記憶し(4024)、サーバ1000のサーバ電源遮断を行う。利用者がサーバ遮断要求4021を行わなければ、サーバ電源遮断4025は行われない。サーバ電源遮断後は、また図5に示すシーケンスで業務遂行が行われる。

【0063】

図6は、利用者がサーバ1000及びクライアント1001及びストレージデバイス1014を利用するために管理者が行うストレージデバイス1014の初期化操作を説明した図である。図6にて説明される一連の動作は、図5に示した利用者の利用が開始される前もしくは利用者がカードを閉塞もしくは紛失し、利用権限を失った際に行われる。

【0064】

クライアント6000は、クライアント1001と同様にディスプレイやユーザインターフェースやリーダライタを接続されたクライアントで、管理者がストレージデバイス1014の書き込みを行うために利用する。

【0065】

まず、管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント6000を通じ、サーバ1000に登録することにより、サーバ1000より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う(6001)。ここで、ストレージデバイス1014は、既にストレージデバイス供給者から鍵証明書格納プログラム2046などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス1014もしくはクライアント6000もしくは管理者が別途生成した秘密鍵に対応する公開鍵を6001にて送付することにより得られる。作成された認証情報と公開鍵証明書は、クライアント6000を経由してストレージデバイスへ書き込まれる(6002)。次に管理者は、ストレージデバイス1014内の認証情報と鍵の利用権をコントロールするための情報を変更する(6003、6004)。この操作によってストレージデバイス1014は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

【0066】

次に、管理者は、ソフトウェア機能の書き込みを行い、ソフトウェア機能は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ2012、デバイス管理用ツール2013、デバイスドライバ2014、インターフェースハンドラ2015、インストーラ2016、遠隔操作端末用アプリケーション2017、暗号化通信路構築用アプリケーション2018、業務アプリケーション2019などである。

【0067】

次に、管理者は、サーバ接続試験要求(6007)を行い、サーバ接続試験が行われる(6008)。サーバ接続試験6008は、図5にて示した利用者が行うサーバへの接続や業務遂行のプロセスを管理者が行い、ストレージデバイス1014内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス1014は、利用者に送付される。この際、ストレージデバイス1014は利用者のIDや顔写真や氏名などを印刷されるか、シール針付けするなどされる。また、ストレージデバイス1014を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス1014を送付するのとは別の封書などの方法で利用者に送付される。

【0068】

図11は、本実施例のクライアント1001上で動作するミドルウェアについて説明した図である。クライアント1001上で動作する遠隔操作端末用アプリケーション2017や暗号化通信路構築用アプリケーション2018、業務アプリケーション2019のようなアプリケーション11000は、図示するように2つの経路を利用してリーダーライタ1012及びストレージデバイス1014にアクセスを行う。カード内のファイルアクセスやファイル管理を行いたい場合は、ファイルアクセス用API11001、ファイルアクセス用ドライバ11002、リーダーライタ1012内のリーダーライタファームウェア11003を経由し、ストレージデバイス1014内のカードOS及びアプリケーション11004が呼び出される。また、カード内の耐タンパデバイス2032に命令を発するなど、セキュリティ認証にかかわる命令を実行したい場合は、インターフェースハンドラ3015、デバイス3014、リーダーライタ1012内のリーダーライタファームウェア11003を経由し、ストレージデバイス1014内のカードOS及びアプリケーション11004が呼び出される。この際、ファイルアクセス用ドライバ11002、リーダーライタファームウェア11003、デバイス3014は、お互いの命令が同時に発生することが無いように常にストレージデバイス1014とリーダーライタ1012のアクセス状態を監視し、ストレージデバイス1014に対して適切なアクセスがなされるように、自身で命令のストックや拒否などの輻輳制御を行う。

【0069】

図13は、デバイスドライバ3014とファイルアクセス用ドライバ11002の行う輻輳制御をフローチャートを用いて説明した図である。ドライバ3014及び11002は、OSの起動時などに初期化され、処理が開始される(13000)。ファイルアクセス用ドライバ11002への要求もしくは待機した要求があるかどうかチェックが行われ(13001)、要求があった場合、リーダーライタを介したカードへのファイルアクセスが行われる(13002)。次に、デバイスドライバ3014への要求があるかどうかのチェックが行われる(13003)。ある場合は、リーダーライタを介したCPU2030へのアクセスが行われる(13004)。ファイルアクセス用ドライバ11002への要求がこの時点であるかどうかチェックが行われ(13005)、要求があった場合、ファイルアクセス用ドライバ11002への要求待機処理が行われる。この要求待機処理は、ファイルアクセス用ドライバ11002において行われ、要求待機用に作られたメモリ領域に、待機すべき要求がストックされる。ストックされた要求は、次に処理13002が実行される際に処理される。ただし、処理13002により処理が行われるまでのストックしている時間があらかじめ定めた一定量を超えた場合は、処理13005内で、アプリケーションへタイムアウトなど異常を通知し、処理を破棄する。デバイスドライバ301

また、本実施の形態では、クライアント 1 0 0 1 及びサーバ 1 0 0 0 を別の構成として記載したが、逆にクライアント 1 0 0 1 がサーバ 1 0 0 0 の機能を兼ねたり、サーバ 1 0 0 0 をクライアント 1 0 0 1 の代わりに使用したりすることが可能でもよい。また、サーバ 1 0 0 0、クライアント 1 0 0 1、1 0 0 2 は、P C や P e r s o n a l D i g i t a l A s s i s t a n t s (P D A)、ワークステーションであるように記載したが、高性能複写機、現金自動支払機 (A T M)、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生 (録音) 装置、販売時点商品管理システム、街角端末、I n t e l l i g e n t T r a n s p o r t S y s t e m s (I T S) 用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。

【実施例 2】

【 0 0 7 7 】

図 7 から図 9 用いて、本発明に係るセキュアリモートアクセスシステムの第 2 の実施形態を説明する。

【 0 0 7 8 】

図 7 は、本発明の第 2 の実施形態のリモートアクセスシステムを示す図である。

【 0 0 7 9 】

利用者の使用するサーバ 1 0 0 0 とクライアント 1 0 0 1、ストレージデバイス 1 0 1 4 は、第 1 の実施形態にて説明したものと同様である。ゲートウェイ 7 0 0 0 は、クライアント 1 0 0 1 とサーバ 1 0 0 0 の通信の暗号化と利用者、利用機器認証を行う中継機器である。

【 0 0 8 0 】

ゲートウェイ 7 0 0 0 は、一般的にファイアーウォール、暗号化ゲートウェイ、バーチャルプライベートネットワーク (V P N) ゲートウェイなどと呼ばれる。本実施例では、ゲートウェイ 7 0 0 0 は、ファイアーウォールと暗号通信機能をインストールされたサーバ機であるとして説明を行うが、例えば、ネットワークルータや無線 L A N アクセスポイント、ネットワークハブ、ブロードバンドルータなどでも良い。ネットワーク 7 0 0 1 は、例えばインターネットや地域 I P ネットワークのような、公衆回線であり、ネットワーク 1 0 0 6 より通信内容の盗聴や改ざんの危険性の高いネットワークである。クライアント 1 0 0 1 は、ネットワーク 7 0 0 1 越しにサーバ 1 0 0 0 を遠隔操作するため、ゲートウェイ 7 0 0 0 とクライアント 1 0 0 0 の間にて暗号通信と暗号通信を行うための認証を行う。

【 0 0 8 1 】

ゲートウェイ 7 0 0 0 は、C P U 7 0 0 2、メモリ 7 0 0 3、ストレージ 7 0 0 4 を持ち、動作時にストレージ 7 0 0 4 内に設定された暗号通信及び認証用アプリケーションがメモリ 7 0 0 3 にロードされ C P U 7 0 0 2 にて通信の制御を行う。ゲートウェイ 7 0 0 0 は、認証用サーバ 7 0 0 5 に直接もしくはネットワークを経由して接続している。認証用サーバ 7 0 0 5 は、ゲートウェイ 7 0 0 0 にて暗号通信を行う際の認証情報を蓄積し、ゲートウェイ 7 0 0 0 の問合せに対して応答したり、接続されたリーダライタ 7 0 0 7 を介して、ストレージデバイス 1 0 1 4 の初期化や活性化、個人化などを行う。認証用サーバ 7 0 0 5 は、内部認証局を持っても良いし、外部の認証局の証明書リストや証明書リボケーションリストを管理し、ゲートウェイ 7 0 0 0 に通知する役割だけを持っても良い。

【 0 0 8 2 】

図 8 に、本実施形態のリモートアクセスシステムを利用する際のストレージデバイス 1 0 1 4 の初期化と利用者がクライアント 1 0 0 1 にストレージデバイス 1 0 1 4 を挿入し、サーバ 1 0 0 0 を利用する際の管理者、利用者、ストレージデバイス 1 0 1 4、クライアント 1 0 0 1、ゲートウェイ 7 0 0 0、サーバ 1 0 0 0 間にて行われる通信の詳細を示した図を示す。

【 0 0 0 0 】

管理者は、ストレージデバイス 1 0 1 4 を認証サーバ 7 0 0 5 と通信が可能なリーダライタ 7 0 0 7 に挿入する。管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント 1 0 0 1 を通じ、認証サーバ 7 0 0 5 に登録することにより、認証サーバ 7 0 0 5 より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う（8 0 0 1）。ここで、ストレージデバイス 1 0 1 4 は、既にストレージデバイス供給者から鍵証明書格納プログラム 2 0 4 6 などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス 1 0 1 4 もしくは認証サーバ 7 0 0 5 もしくは管理者が別途生成した秘密鍵に対応する公開鍵を 8 0 0 1 にて送付することにより得られる。作成された認証情報と公開鍵証明書は、ストレージデバイス 1 0 1 4 へ書き込まれる。次に管理者は、ストレージデバイス 1 0 1 4 内の認証情報と鍵の利用権をコントロールするための情報を変更する（8 0 0 3、8 0 0 4）。この操作によってストレージデバイス 1 0 1 4 は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

【 0 0 8 4 】

次に、管理者は、アプリケーションの書き込み要求を行い、認証サーバ 7 0 0 5 は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ 2 0 1 2、デバイス管理用ツール 2 0 1 3、デバイスドライバ 2 0 1 4、インターフェースハンドラ 2 0 1 5、インストーラ 2 0 1 6、遠隔操作端末用アプリケーション 2 0 1 7、暗号化通信路構築用アプリケーション 2 0 1 8、業務アプリケーション 2 0 1 9 などである。

【 0 0 8 5 】

次に、管理者は、サーバ接続試験要求（8 0 0 7）を行い、サーバ接続試験が行われる（8 0 0 8）。サーバ接続試験 8 0 0 7 は、ストレージデバイス 1 0 1 4 内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス 1 0 1 4 は、利用者に送付される（8 0 0 9）。この際、ストレージデバイス 1 0 1 4 を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス 1 0 1 4 を送付するのとは別の封書などの方法で利用者に送付される。

【 0 0 8 6 】

次に、利用者はクライアント 1 0 0 1 の利用を開始するまでに利用者の認証情報やクライアント 1 0 0 1 を動作させるためのアプリケーションが保存されたストレージデバイス 1 0 1 4 をクライアント 1 0 0 1 のリーダライタに接続する。利用者が、クライアント 1 0 0 1 を利用したことがない場合は、利用者はストレージデバイス 1 0 1 4 内のインストーラ 2 0 1 6 を利用し、デバイスドライバ 2 0 1 4 やデバイス管理ツール 2 0 1 3 や遠隔端末用アプリケーション 2 0 1 7 のようなサーバ 1 0 0 0 を操作するために必要な情報もしくはアプリケーションをクライアント 1 0 0 1 にインストールする。この際、クライアント 1 0 0 1 によってストレージデバイス 1 0 1 4 から直接実行できるアプリケーションのインストールを行う必要はない。

【 0 0 8 7 】

利用者は、まずシーケンス 8 0 1 0 に示すようにクライアント 1 0 0 1 にゲートウェイ接続要求を行う。クライアント 1 0 0 1 はゲートウェイ 7 0 0 0 にサーバ動作確認を行う（8 0 1 1）ゲートウェイ 7 0 0 0 のリモート機器からのログインに対するセキュリティポリシーの設定によるが、利用者の認証を P K I を用いた認証が必要もしくは可能である場合、ゲートウェイ 7 0 0 0 からの認証情報の要求（8 0 1 2）、クライアント 1 0 0 0 からの証明書の要求（8 0 1 3）、ストレージデバイス 1 0 1 4 からの証明書の送信（8 0 1 4）、クライアント 1 0 0 1 からの署名の要求（8 0 1 5）が行われる。ストレージ

、サーバ1014において省スペース化、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。本実施例では、暗証番号を利用した例を示す。ストレージデバイス1014からの暗証番号要求(8016)が行われた後、クライアント1001から利用者へ暗証番号要求表示(8017)がディスプレイ1008などを利用して行われる。利用者が暗証番号をユーザインターフェース1010とクライアント1001を介してストレージデバイス1014に送信すると(8018、8019)、ストレージデバイス1014内のCPU2001もしくはCPU2030においてサーバ1000、クライアント1001から送信された情報に対し、秘密鍵2040のうちの一つもしくはいくつかを用いた電子署名が作成される(8020)。作成された署名は、クライアントに送信される(8021)。クライアント1001は、証明書2010、2043などの認証情報と作成された署名の送信を行う(8022)。次に、サーバ1000及びクライアント1001は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う(8023)。この鍵交換8023は、暗号化通信路構築用アプリケーション2018により行われる。シーケンス8023において交換された秘密共有鍵を用いて、ゲートウェイ7000及びクライアント1001は暗号化通信路を構築し、2者の間で通信される情報は暗号化される。

【0088】

次に、利用者は、シーケンス8030に示すようにクライアント1001に動作確認要求を行う。クライアント1001はサーバ1000にサーバ動作確認を行う(8031)利用者はサーバ1000の動作を確認できなかった場合は、ストレージデバイス1014もしくはインストラ2016にてクライアント1001上に用意された遠隔地からサーバの電源を投入するLANを利用して機器の電源投入を行うようなWake up on LANのような機能を利用してサーバ1000の電源投入を行う。この場合、サーバ1000の、ネットワークに対するI/Fは常時通電されており、IDとパスワードのセットやネットワークボードのMACアドレス等、何らかの認証情報を利用してサーバ1000の起動が行われる(8032、8033)。この操作によりサーバ1000は起動される(8034)。サーバの起動が完了した際、利用者はクライアント1000にログイン要求を入力する(8035)。この操作は、クライアント1000内の遠隔操作アプリケーション2017により行われる。遠隔操作アプリケーションがインストールされていない場合、この時点にてクライアント1001にロードされる。サーバ1000のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証をPKIを用いた認証が必要もしくは可能である場合、サーバ1000からの認証情報の要求などが行われ、8012～8023と同様の署名の作成と送信がサーバ1000に対し行われる。利用者は、ゲートウェイ7000において強固な認証を通過しているので、サーバ1000がゲートウェイ7000からの通信を信頼できるとすると、ログイン要求8035を行う際のサーバ1000の認証はIDとパスワード認証などの簡便なものでも良い。

【0089】

暗号化通信路構築とサーバ1000へのログインが完了した段階で、ユーザは、サーバ1000または、クライアント1001、ストレージデバイス1014上に保存されているアプリケーションを起動し、業務遂行をする(8036)。

【0090】

業務遂行中は、CPU2001もしくはCPU2030もしくはサーバ1000もしくはクライアント1001は、ログ情報2011、2042、3011に情報を追記し、利用者の業務遂行を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス1014やクライアント1001内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ1000に送信される。

【0091】

利用者の利用するサーバ1000の管理を行う管理者は、ログ情報2011、2042

、3011の情報をサーバ1000に返送される情報を監視し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク1006を介した異常なアクセス、クライアント1001内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ1000もしくはクライアント1001もしくは、ストレージデバイス1014の利用を停止するようなオペレーションとは、サーバ1000及びクライアント1001への利用者のログインの禁止や電源遮断、ストレージデバイス1014の閉塞などが該当する。ストレージデバイス1014の閉塞とは、PIN検証プログラム2045の利用する情報を変更し、利用者がストレージデバイス1014を利用できないようにすることである。利用者の業務など、サーバ1000の利用が終了した場合、利用者は、クライアント1001に対しサーバ遮断要求を行う(8037)。サーバ遮断要求はクライアント1001からサーバ1000に送信される(8038)。サーバ1000及びクライアント1001はセッションの遮断8039を行う。サーバ1000は、利用者の利用情報のログをサーバ1000上に記憶し(8040)、サーバ1000のサーバ電源遮断を行う。利用者がサーバ遮断要求8037を行わなければ、サーバ電源遮断8041は行われない。サーバ電源遮断後は、また8010以降のシーケンスで業務遂行が行われる。

【0092】

図9に、本実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図を示す。図中9000にて示されたネットワークとネットワークに接続した機器のグループは、利用者が中心的に利用するネットワークと機器のグループである。ネットワークと機器のグループ9000は、例えば、利用者が常に勤務するオフィスのローカルエリアネットワーク(LAN)とLANに接続された機器である。9000内には、ユーザの利用可能なサーバ1000、クライアント1002、部門サーバ9001、PC9002、ゲートウェイ9006、7000、認証サーバ7005がLAN9003を中心に接続されている。また、9010にて示されたネットワークとネットワークに接続した機器のグループは、利用者が出張時などに利用する所属外の事業部などのWAN上のネットワークと機器のグループである。9010内には、ユーザの利用可能なクライアント9008、ゲートウェイ9007がネットワーク9005を中心として接続されている。また、ネットワーク7001のような社外のネットワークにルータ9004を介してクライアント1001が接続されている。

【0093】

ここで、利用者は、ストレージデバイス1014を持ち歩くことにより、LAN上のクライアント1002、WAN上のクライアント9008、インターネットを介しLAN9003に接続しているクライアント1001を利用して、LAN9003と接続されたサーバ1000、部門サーバ9001、PC9002を利用することができる。この際、LAN上のクライアント1002、WAN上のクライアント9008からLAN9003と接続されたサーバ1000、部門サーバ9001、PC9002を利用する際は、ゲートウェイ9007、9006では、通信の暗復号を行わず、ゲートウェイ7000を利用する場合、通信の暗復号を行うようにすれば、利用者の利用手順の簡略化を図りつつ、通信内容の秘匿が可能である。ここで、部門サーバ9001とは、LAN上に設置されたウェブサーバやメールサーバやリモートログインして演算を行うターミナルサーバなどを示す。PC9002は、利用者の所属する部門が共有などで利用している共有リソース管理用PCや出張者用貸し出しPCなどを示す。

【0094】

上記のように、本実施形態に示したクライアント1001は、耐タンバストレージ機能を搭載したストレージデバイス1014を挿入しサーバ1000、部門サーバ9001、PC9002などを遠隔操作することにより、利用者に安全で、使い勝手良く利用できる業務システムを構成することが可能となる。

また、利用者は、利用するクライアント 1 0 0 1 からクライアント 1 0 0 2、9 0 0 8 に変更したとしても、様々な異なる業務執行場所において、クライアント 1 0 0 1 を利用するのと同様の操作感覚にて業務遂行を行うことができるため、利用者の使い勝手が向上する。

また、サーバ 1 0 0 0、クライアント 1 0 0 1、1 0 0 2、9 0 0 8 は、P C や P D A、ワークステーションであるように記載したが、高性能複写機、A T M、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生（録音）装置、販売時点商品管理システム、街角端末、I T S 用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。

【実施例 3】

【 0 0 9 6 】

図 1 0 を用いて、本発明に係るセキュアリモートアクセスシステムの第 3 の実施形態を説明する。

【 0 0 9 7 】

図 1 0 は、本発明の第 3 の実施形態を示すリモートアクセスシステムを示す図である。

【 0 0 9 8 】

利用者の使用するサーバ 1 0 0 0 0 は、サーバ 1 0 0 0 と同等の機能をもつ複数のサーバ（P C）の集合体である。サーバ 1 0 0 0 0 はサーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 上にある、それぞれ C P U 1 0 0 3 0、1 0 0 4 0、…、1 0 0 5 0、メモリ 1 0 0 3 1、1 0 0 4 1、…、1 0 0 5 1 により動作する。図 1 0 では、利用者は、サーバ 1 0 0 3 2 を利用し、C P U 1 0 0 3 0 上にて実行された情報をディスプレイ 1 0 0 8 に出力させて業務を遂行している。サーバ 1 0 0 0 0 は、切り替え器 1 0 0 0 4 を利用してサーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 と接続するユーザインターフェース 1 0 0 0 3 及びディスプレイ 1 0 0 0 2 を選別している。また、サーバ 1 0 0 0 0 は、制御装置 1 0 0 0 1 に接続されている。制御装置 1 0 0 0 1 は、ネットワーク 1 0 0 5 に接続しており、サーバ 1 0 0 0 0 と同様にストレージデバイス 1 0 1 4 を持つ適切な利用者が利用可能である。ここで、利用者がサーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 のいずれかを利用しようとした際に、制御装置 1 0 0 0 1 は、サーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 の電源管理、電源のオンオフ、状態のクライアントへの通知を行う。特に、クライアント 1 0 0 1 からのサーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 への通信が不通になった際は、利用者は、制御装置 1 0 0 0 1 にログインし、サーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 の状態を確認したり、電源をオンオフしたりする。制御装置 1 0 0 0 1 内にはハードディスクやフラッシュメモリなどのサーバブート用のストレージが実装しており、このストレージ上のデータを用いてサーバ 1 0 0 3 2 ～ 1 0 0 5 2 がブートアップする。このことにより、利用者のサーバ管理の工数が減少する。

【 0 0 9 9 】

上記のように、本実施形態に示したサーバ 1 0 0 0 0 及び制御装置 1 0 0 0 1 を、耐タンバストレージ機能を搭載したストレージデバイス 1 0 1 4 を挿入したクライアント 1 0 0 1 より利用することにより、サーバ 1 0 0 0 0 は、1 つの筐体の内部に複数の類似した機能を持つサーバを持つ特長から、管理者のサーバ 1 0 0 3 2、1 0 0 4 2、…、1 0 0 5 2 の管理工数を削減することができる。また、利用者が制御装置 1 0 0 0 1 を利用することによりサーバの電源管理などが容易に行えるため、利用者の使い勝手が向上する。

【図面の簡単な説明】

【 0 1 0 0 】

【図 1】 本発明の第 1 の実施形態のセキュアリモートアクセスシステムを説明するためのブロック構成図。

【図 2】 本発明の第 1 の実施形態のストレージデバイスを説明するためのブロック構成図。

【図 3】 本発明の第 1 の実施形態の認証情報のフローの構成を示す図。

【図 4】 本発明の第 1 の実施形態のクライアントの詳細を示したブロック構成図

【図 5】 本発明の第 1 の実施形態の利用者、ストレージデバイス、クライアント、サーバ間にて行われる通信の詳細を示した図

【図 6】 本発明の第 1 の実施形態の管理者が行うストレージデバイスの初期化操作を説明した図

【図 7】 本発明の第 2 の実施形態のリモートアクセスシステムを示す図

【図 8】 本発明の第 2 の実施形態の利用者、管理者、ストレージデバイス、クライアント、ゲートウェイ、サーバ間にて行われる通信の詳細を示した図

【図 9】 本発明の第 2 の実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図

【図 10】 本発明の第 3 の実施形態を示すリモートアクセスシステムを示す図

【図 11】 本発明の第 1 の実施形態のソフトウェア構成を示す図

【図 12】 本発明の第 1 の実施形態のアプリケーションから一時記憶領域を利用する際の処理方法を示すフローチャート

【図 13】 本発明の第 1 の実施形態のドライバにおける輻輳制御を行う際の処理方法を示すフローチャート

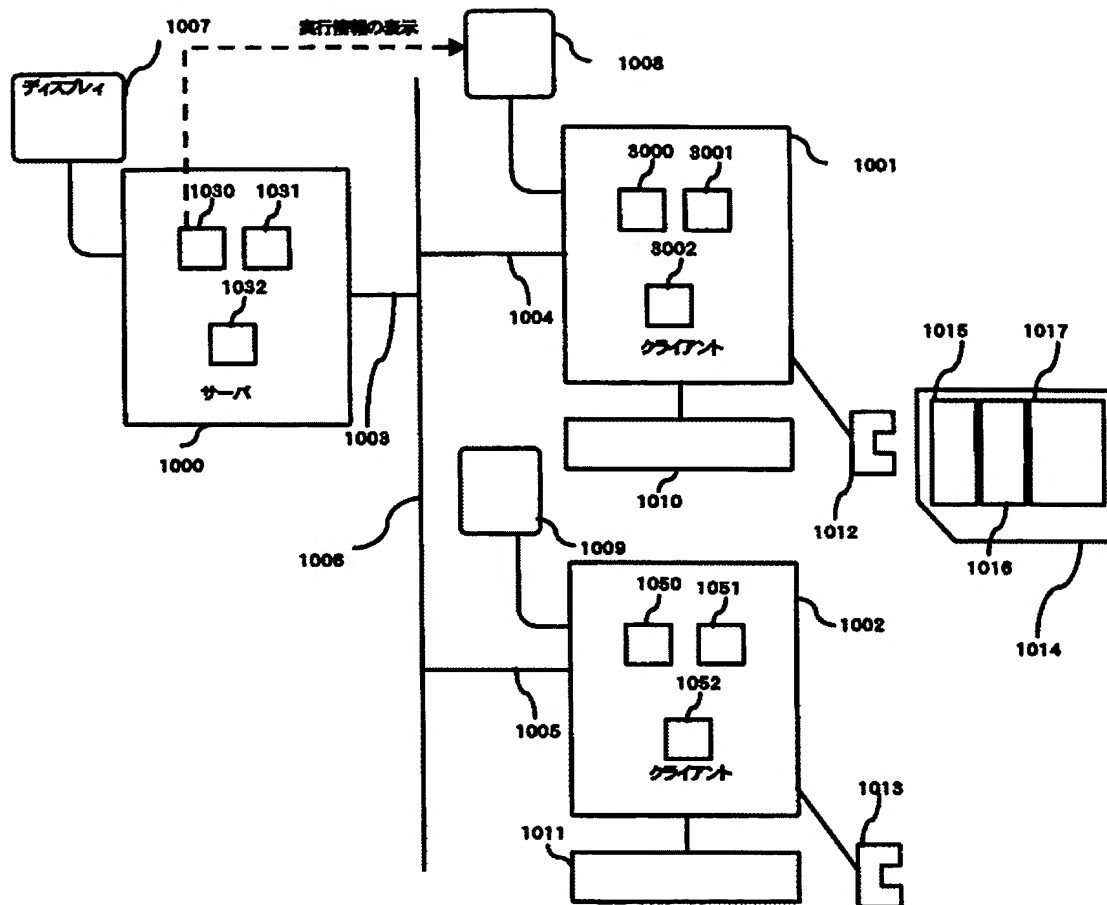
【図 14】 本発明の第 1 の実施形態のドライバにおける輻輳制御を示すタイムチャート

【符号の説明】

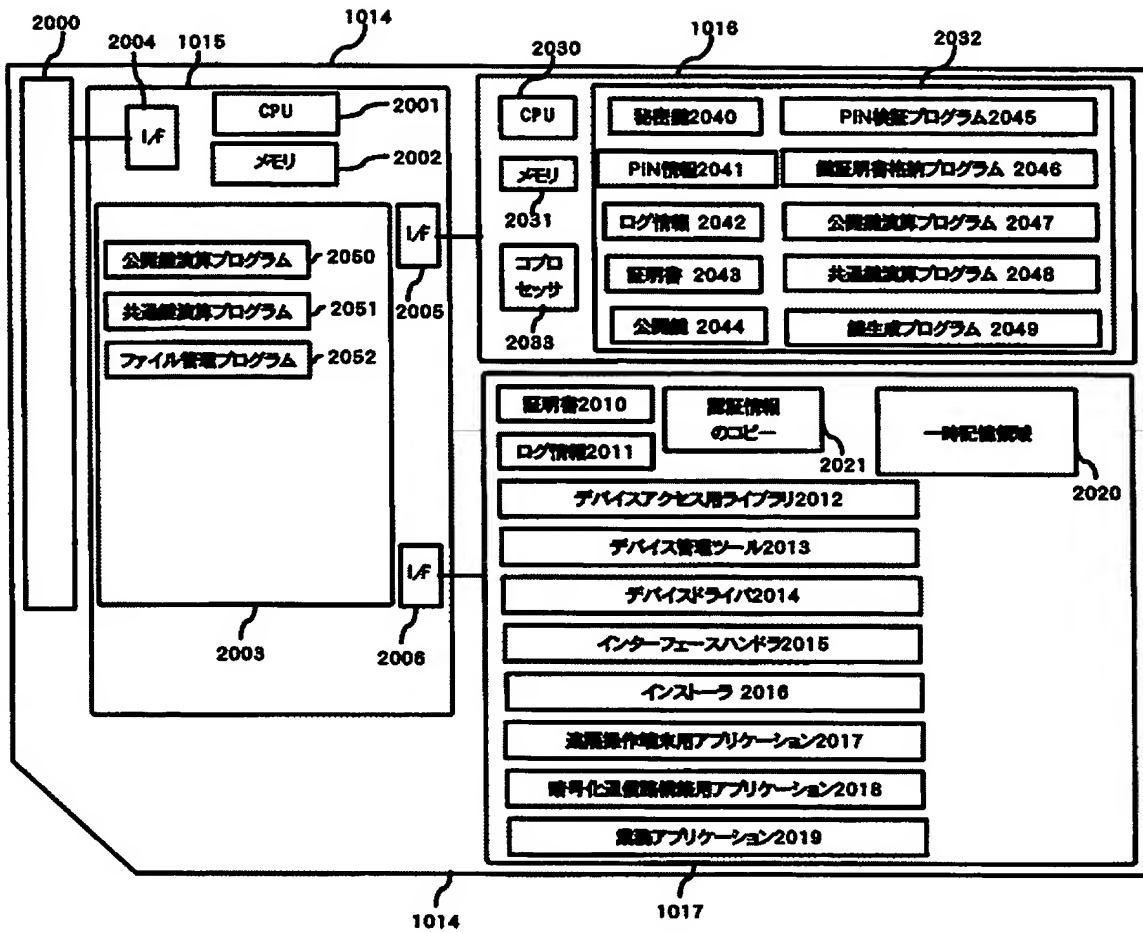
【0101】

1000…サーバ、1001、1002…クライアント、1003、1004、1005
…ネットワークケーブル、1006…ネットワーク、1007、1008、1009、1
0002…ディスプレイ、1010、1011、10003…ユーザインターフェース、
1012、1013…リーダーライター、1014…ストレージデバイス、1015…コント
ローラ、1016…耐タンパデバイス、1017、1032、1052、2032、30
02、7004…ストレージ、1030、1050、2001、2030、3000、7
002、10030、10040、10050…CPU、1031、1051、2002
、2031、3001、7003、10031、10041、10051…メモリ、20
00…端子、2003…不揮発メモリ2003、2004、2005、2006、302
0、3021、3022、3023…インターフェース、2050…公開鍵演算プログラ
ム、2051…共通鍵演算プログラム、2052…ファイル管理プログラム、2040…
秘密鍵、2041…PIN情報、2042…ログ情報、2043…証明書2043、20
44…公開鍵2044、2045…PIN検証プログラム、2046…鍵証明書格納プロ
グラム、2047…公開鍵演算プログラム、2048…共通鍵演算プログラム、2049
…鍵生成プログラム、5001…証明書1、5002…証明書2、5003…証明書N、
5004…ミドルウェアの認証情報、3010…証明書、3011…ログ情報、3012
…デバイスアクセス用ライブラリ、3013…デバイス管理用ツール、3014…デバイ
スドライバ、3015…インターフェースハンドラ、3016…遠隔操作端末用アプリケー
ション、3017…暗号化通信路構築用アプリケーション、3018…業務アプリケー
ション、7000…ゲートウェイ、7001…ネットワーク、7005…認証用サーバ、
7007…リーダーライター、9001…部門サーバ、9002…PC、9003…LAN、
9004…ルータ、9005…ネットワーク、9006、9007…ゲートウェイ、90
08…クライアント、10000、10032、10042、10052…サーバ、10
001…制御装置、10004…切り替え器、11000…アプリケーション、1100
1…ファイルアクセス用API、11002…ファイルアクセス用ドライバ、11003
…リーダーライターファームウェア、11004…カードOS及びアプリケーション。

【 図 1 】

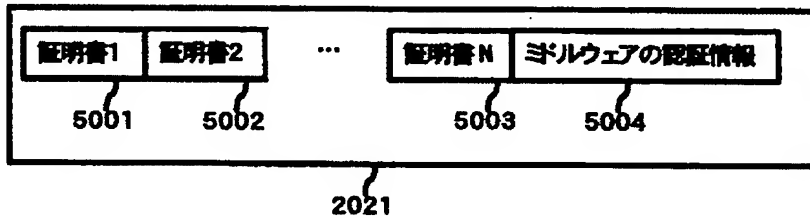


【図 2】

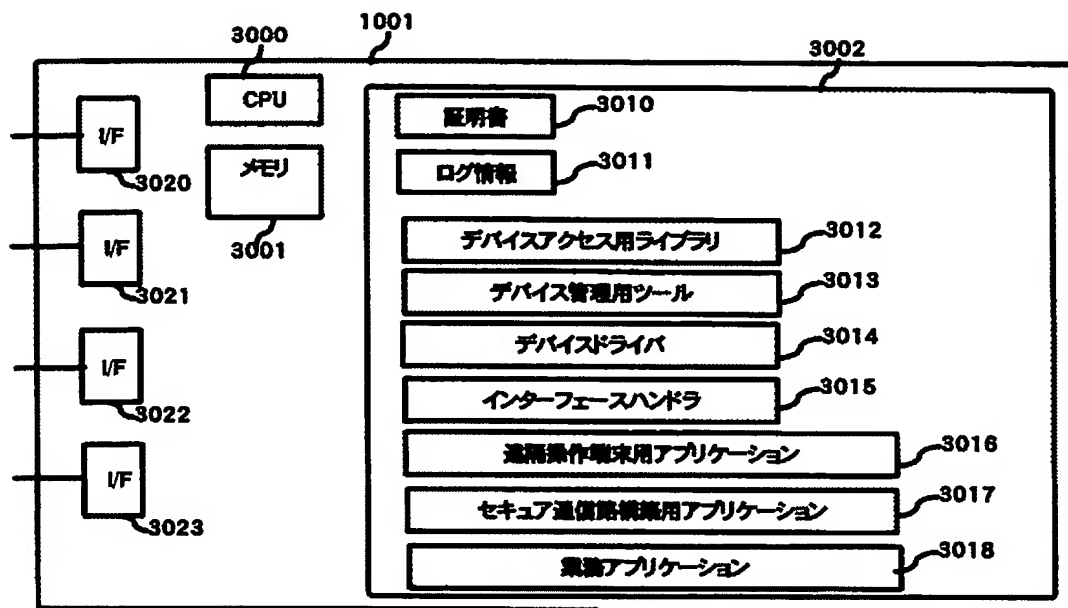


【図 3】

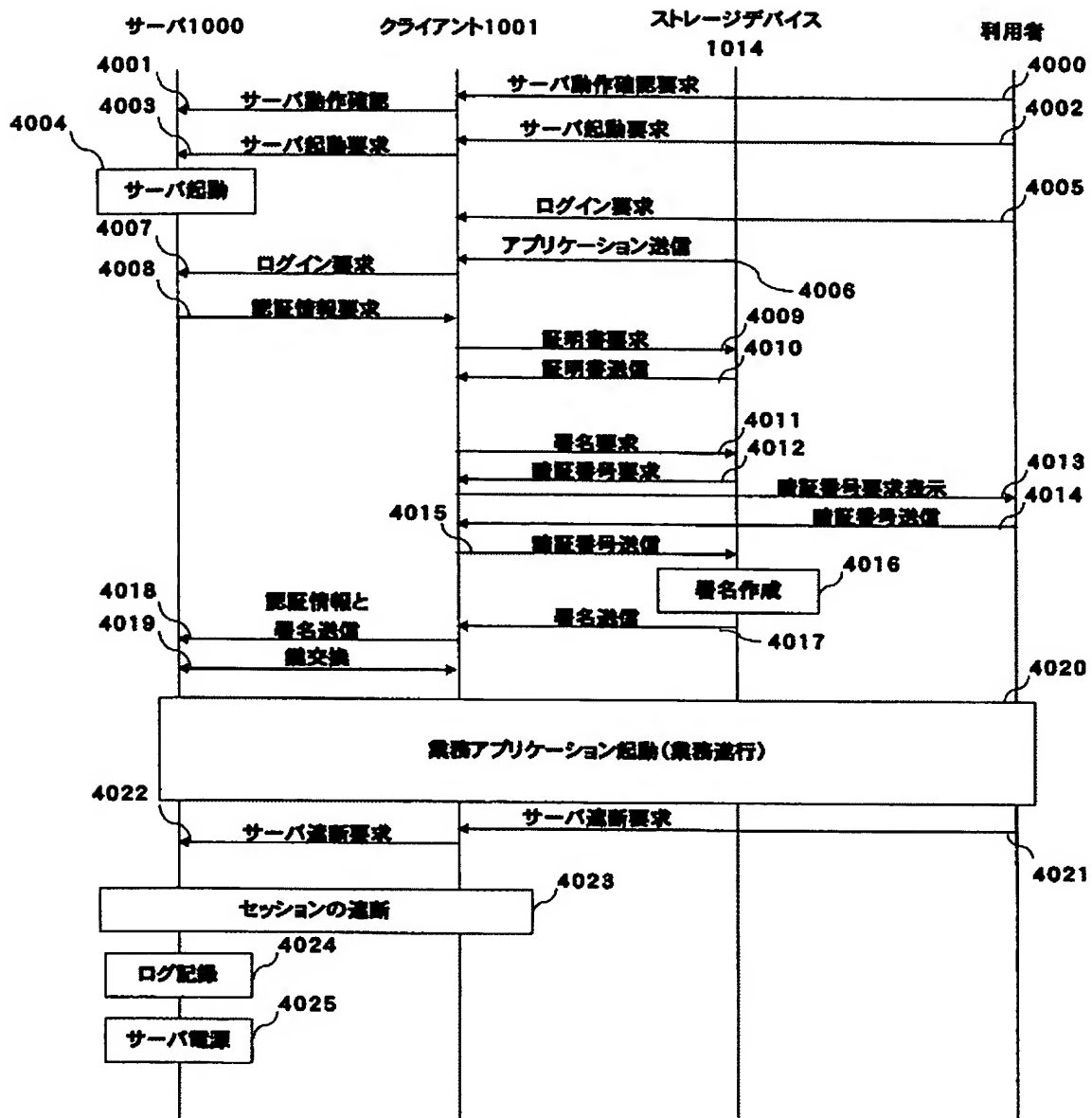
【図 3】



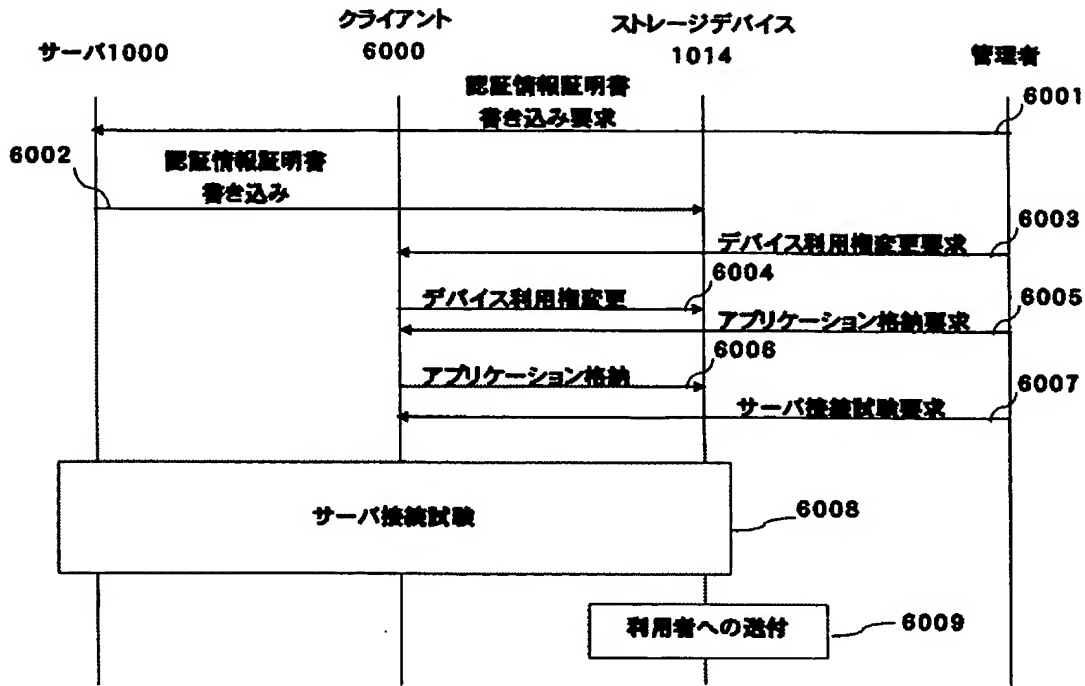
【図 4】



【図5】

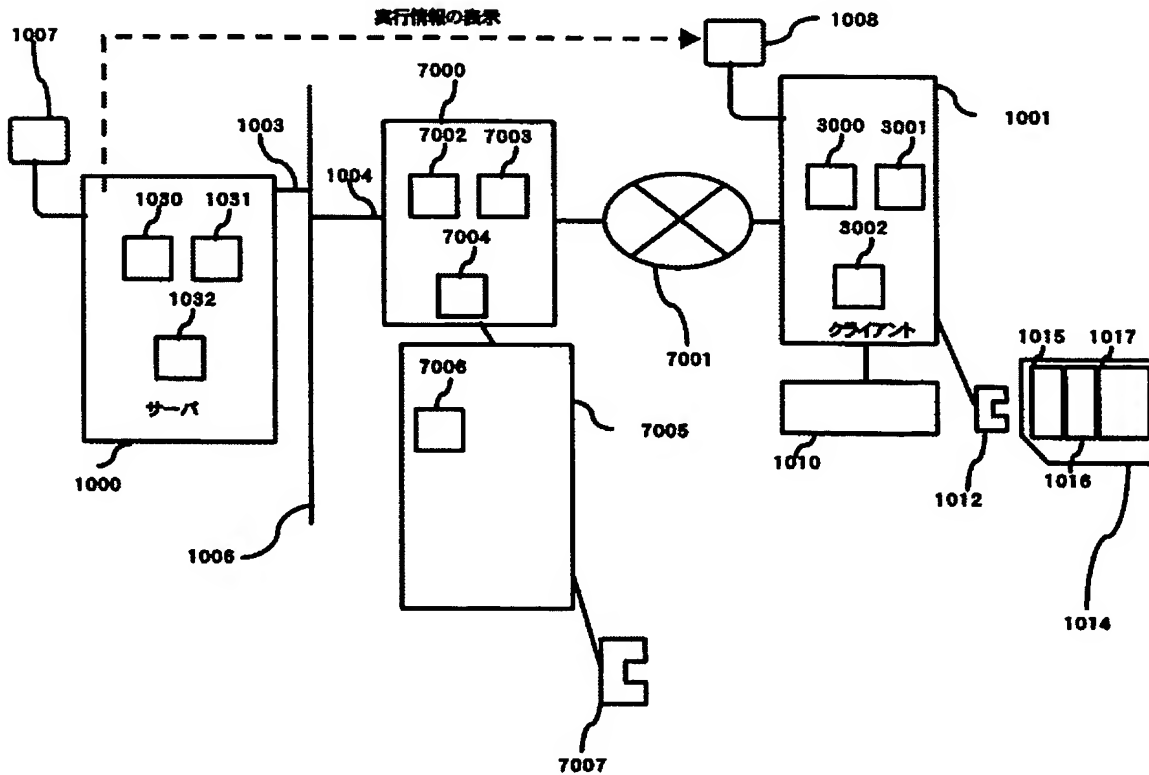


【図6】

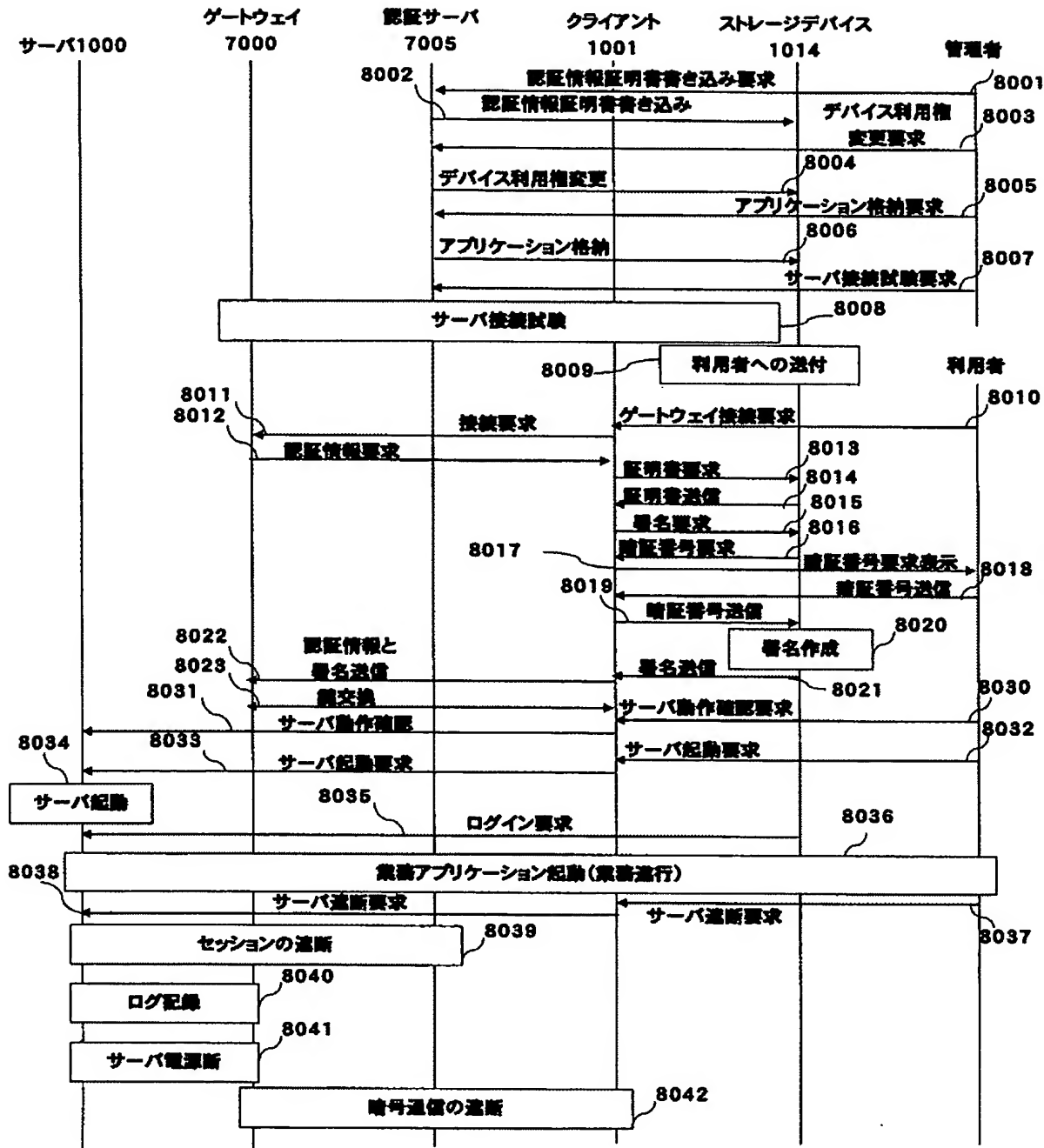


【図7】

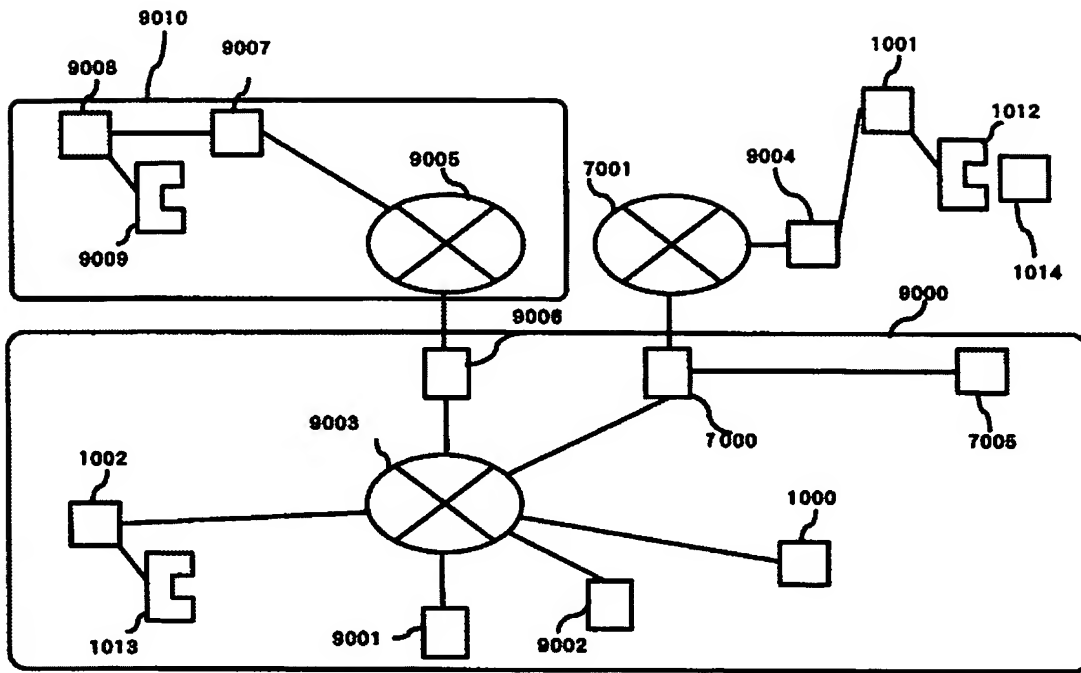
【図7】



【図8】

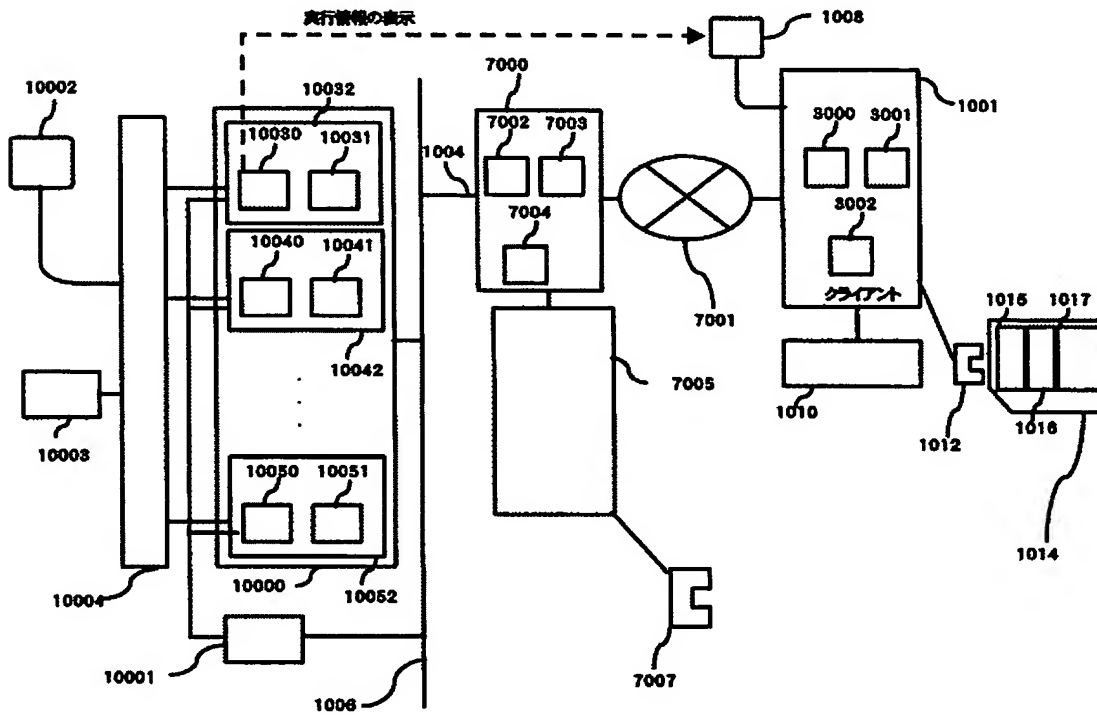


【 図 9 】

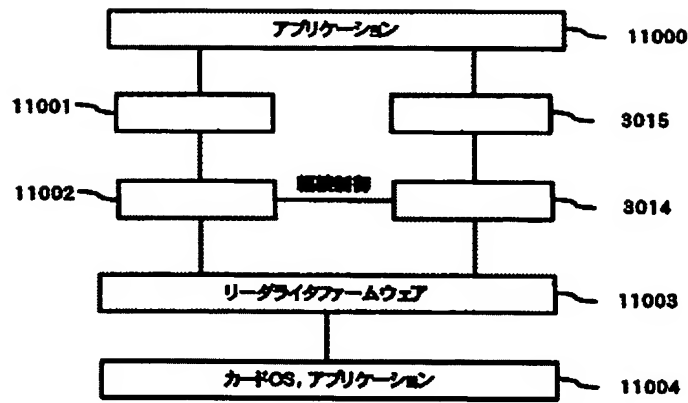


【 図 10 】

【 図 10 】

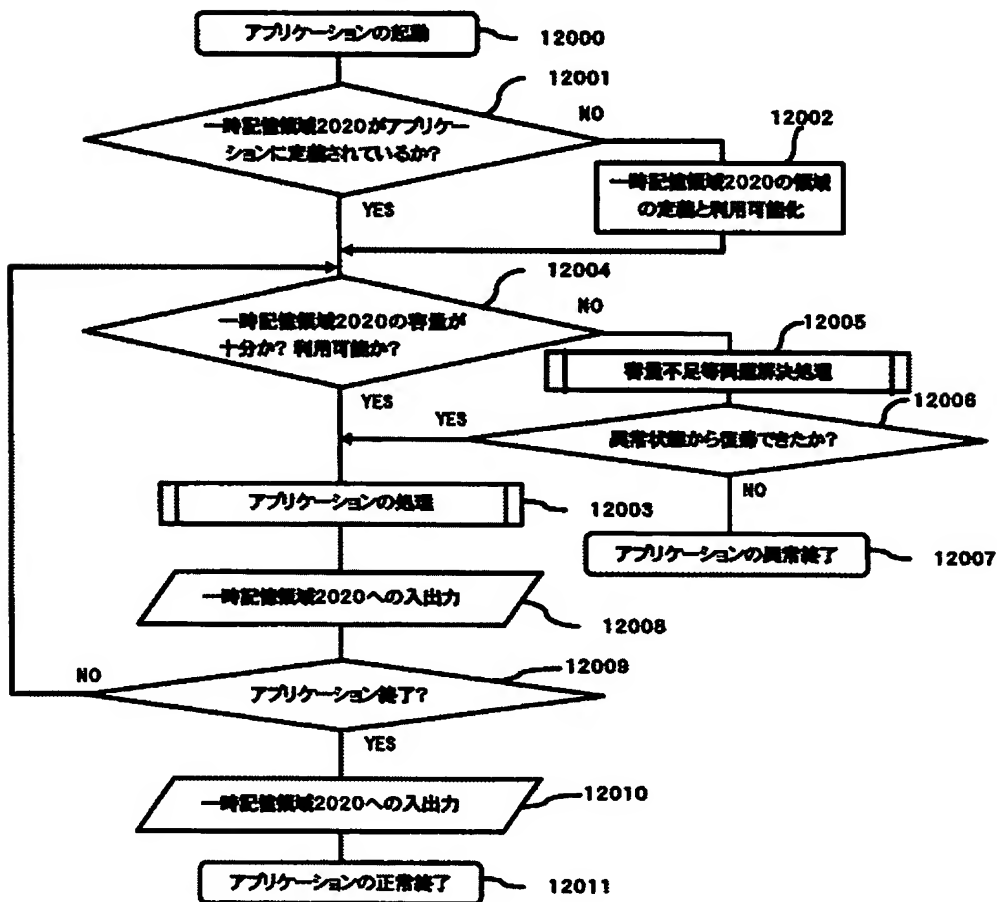


【図 1 1】

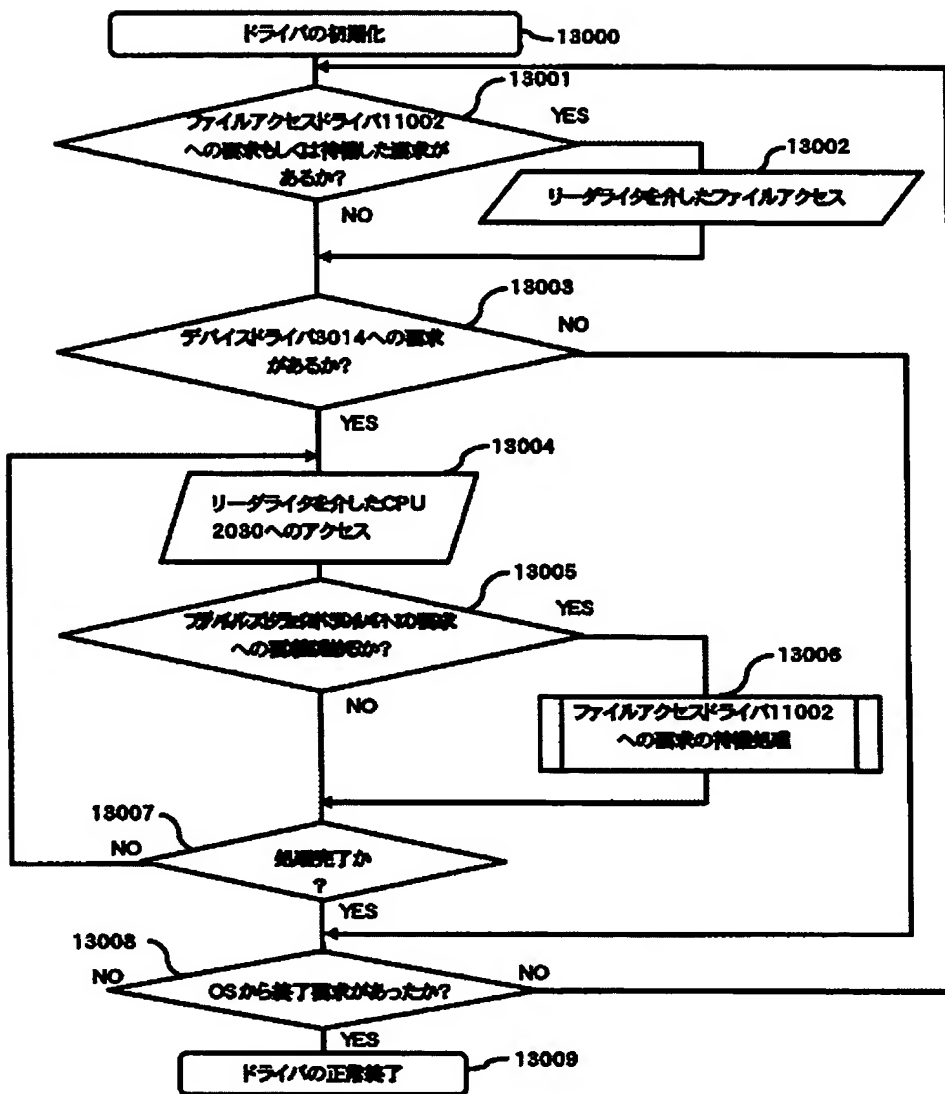


【図 1 2】

【図 1 2】

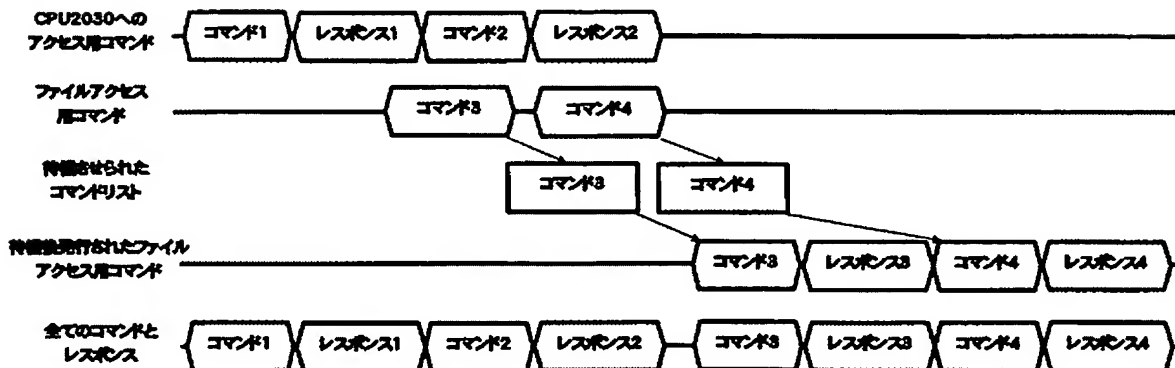


【図13】



【図14】

【図14】



【要約】

【課題】 利用者が不特定のクライアントからサーバに対し暗号通信を行いながらアクセスし、業務遂行を行うセキュアリモートアクセスシステムにおいて、利用者の認証デバイスとして耐タンパデバイスを内蔵するストレージデバイスを利用することにより、利用者の利便性を向上させるセキュアリモートアクセスシステムを提供する。

【解決手段】 認定された耐タンパデバイス搭載したストレージデバイスを利用者に配布し、利用者がストレージデバイスを不特定のクライアントに接続し、ストレージデバイス内の認証情報とアプリケーションを用いてサーバを遠隔操作するサーバクライアントシステムを提供することにより、利用者の使い勝手を向上することが可能で、結果としてシームレスに職場内外での業務遂行機能を利用でき、かつ操作したクライアント内に残る機密情報を低減することにより、ユーザのクライアント利用時のセキュリティ及び利便性を向上させるリモートアクセスシステムを提供できる。

【選択図】 図 1

, 0 0 0 0 0 5 1 0 8
19900831
新規登録

東京都千代田区神田駿河台4丁目6番地
株式会社日立製作所
0 0 0 0 0 5 1 0 8
20040908
住所変更

東京都千代田区丸の内一丁目6番6号
株式会社日立製作所

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000698

International filing date: 20 January 2005 (20.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-012594
Filing date: 21 January 2004 (21.01.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse